



April 30, 2012

Proceeding #12-52

Access Comment to FCC Proceeding on Certain Wireless Network Interruptions

Introduction

Access (AccessNow.org) is an international NGO that promotes open and secure access to the internet and telecommunications as a means to the free, full, and safe participation in society and the realization of human rights. Access is committed to protecting internet users' rights no matter where those users reside and, with this Comment, seeks to engage the Federal Communications Commission (the Commission) as a partner in this effort, here in the U.S.

Along with many other stakeholders, at home and abroad, Access was alarmed at the dangerous, unilateral decision by Bay Area Rapid Transit (BART) officials to sever wireless communications on August 11, 2011. As this Comment will make clear, BART's actions were unlawful under the Constitution of the United States. Furthermore, as a heavily regulated semi-public entity, BART's actions conflicted with U.S. treaty obligations under the International Covenant on Civil and Political Rights (ICCPR). Unfortunately, however, the move was not unprecedented.

From Cairo to San Francisco, and London to Côte d'Ivoire, telecommunications providers and their public regulators increasingly encounter human rights considerations, especially involving the freedoms of expression and association, in their operations. Under the United Nations Guiding Principles on Business and Human Rights implementing the Ruggie Framework, all companies must respect human rights and remedy violations, while governments have the responsibility to protect customers, users, and citizens. Without clear guidelines from public authorities like the Commission, however, the telecommunications sector faces particular challenges when navigating emerging issues and responding to stakeholders as diverse as state, regional, and national governments, security services, civil society, consumers, and corporate investors.

Access drew on the Guiding Principles and the ICCPR recently in creating a document, the Telco Action Plan (submitted as an annex to this Comment), outlining principles and implementation objectives for telecommunications companies to better respect human rights and remedy violations. The crux of that Plan, included throughout this Comment, is a test for whether restrictions on the right to freedom of expression violate Article 19 of the ICCPR, regarding the freedoms of expression, opinion, and access to

information. The test derives from one written by the Human Rights Committee, the body that interprets the ICCPR, and its General Comment 34, interpreting Article 19 of the treaty.

In substantial part, the test is as follows: Any limitation on Article 19 rights must be necessary and proportionate to achieve a clearly defined and legitimate public purpose. These terms are strictly construed. Any authority acting to restrict expression “must demonstrate in specific and individualized fashion the precise nature of the threat, and the necessity and proportionality of the specific action taken, in particular by establishing a direct and immediate connection between the expression and the threat.” Security threats cannot be used to justify arbitrary or broad limitations on the right to freedom of expression. Proportionality requires the government to use the least restrictive means necessary to achieve the purported aim.¹

Access firmly believes that, in order to fully respect and protect the rights, freedoms, and safety of citizens, wireless network shutdowns should never occur, and that no government or private official should have authority to order such an interruption under any circumstances. However, we understand that the Commission seeks input and guidance on all aspects of the issue. Thus, we attempt to respond to as many questions in this Comment as possible, but we cannot further the Commission’s inquiry in any manner that assumes an authority to shut down wireless communications should exist.

In this Comment, Access chose to answer those Questions directly relevant to our mandate, including parts of Questions 1, 2, 3, 5, and 6.

1. Past practices and precedents. As noted above, last summer a public agency cited public safety concerns as a reason for temporarily interrupting wireless service on certain portions of a mass transit system. What are examples of previous intentional interruptions of wireless service for public safety reasons, and what policies or rationales have public agencies developed that support or provide guidance on such interruptions?

a. Under what circumstances have public agencies in the United States considered or effectuated interruptions of wireless service for public safety reasons?

¹ Human Rights Committee, General Comment 34, <http://www2.ohchr.org/english/bodies/hrc/docs/CCPR-C-GC-34.doc>; See also the 2011 report of Frank La Rue, Special Rapporteur to the Human Rights Council on the Freedom of Expression, http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf

In 2005, the President's National Security Telecommunications Advisory Committee (NSTAC) (the committee responsible for taking on the subject of massive wireless network shutdowns) reported on a particular instance in the aftermath of the London underground bombings in July 2005. According to the NSTAC annual report, U.S. authorities initiated the complete shutdown of cellular network services in the Lincoln, Holland, Queens, and Brooklyn Battery Tunnels. While the decision was not due to vital security concerns, "...the resulting situation, undertaken without prior notice to wireless carriers or the public, created disorder for both Government and the private sector at a time when use of the communications infrastructure was most needed."²

Following these shutdowns, the National Coordinating Center (NCC) discussed via teleconference the need to streamline a process for determining if and when interruptions of cellular services should be initiated, and what effects they may have, particularly in regard to citizens' ability to access emergency services and more generally, public trust in the reliability of communications infrastructure.

NSTAC then created a task force to recommend a plan for future emergencies that takes into account National Security and "the protection of critical infrastructures," whose recommendations were approved in January 2006.³

Following these events however, there have been a few other examples of communications disruptions. One of which included a move by the US military to block access to certain commercial sites immediately following the earthquake and ensuing tsunami in Japan in 2011, which was done in an effort to ensure that there was sufficient bandwidth available for follow-up military actions.⁴

A situation where a wireless communications crackdown was considered, but not employed, occurred in Philadelphia. In 2010, mobs of young people gathered several times, including on March 20th, when a crowd of 2,000 young people committed vandalism, jumped on cars, and assaulted bystanders. Rather than interrupting communications services, however, local leaders sought to attack the root of the problem, for example, by recognizing the need for more teen programming.⁵

In a related matter, at this very moment there are ongoing discussions about a yet to be tabled bill, which will include an "internet kill switch," giving the President the capability to shut down critical internet infrastructure in certain cases. According to reports, these

² See NSTAC XXIX *Issue Review* here: <http://1.usa.gov/JIXN1Y>

³ NSTAC, Preparedness Directorate (DHS 1-06) (2006) <http://1.usa.gov/lnWmKG>

⁴ <http://edition.cnn.com/2011/US/03/15/us.military.websites>

⁵ Computer World, "Flash mob crackdown in Philly focuses on teens, not technology," <http://bit.ly/94aSBS>

cases would include cyberattacks that would cause more than \$25 billion in damages (in a year), would force mass evacuations, or kill more than 2,500 people.⁶

Access recognizes the need for states to ensure national security, particularly as societies become increasingly connected through the internet and computer systems. Therefore, it is understandable that governments, in very extreme cases of imminent danger to public safety, may have the capacity to temporarily shut down critical infrastructure. However, in any bill that may propose such a measure, the procedure and causes for any shutdown or interruption whatsoever must be consistent with international human rights laws and standards and the rule of law, and necessary and proportionate to achieve a clearly defined and legitimate public purpose. These terms are strictly construed.

Any authority requesting a restriction on expression “must demonstrate in specific and individualized fashion the precise nature of the threat, and the necessity and proportionality of the specific action taken, in particular by establishing a direct and immediate connection between the expression and the threat.” Security threats cannot be used to justify arbitrary or broad limitations on the right to freedom of expression. Proportionality requires the government to use the least restrictive means necessary to achieve the purported aim.⁷

To reiterate, Access is adamantly opposed to any shutdown or throttling of internet and telecommunications services and believes that doing so only undermines and endangers human rights and public safety.

b. What are relevant examples of foreign governments considering or effectuating interruptions of wireless service for public safety reasons? What laws or policies do foreign states have regarding interruption of wireless service for purposes of protecting public safety?

In the past several years there have been myriad examples of governments from around the world who have, or sought to, interfere with communications networks. While many governments claim this is done for reasons of “public safety,” more often than not (and particularly in non-democratic countries), these interruptions are intended to silence speech and/or to quash social and/or political citizen mobilization. The following are some examples of national shutdowns, where communications networks had been

⁶ http://www.usatoday.com/tech/news/internetprivacy/2011-02-15-kill-switch_N.htm

⁷ Human Rights Committee, General Comment 34,

<http://www2.ohchr.org/english/bodies/hrc/docs/CCPR-C-GC-34.doc>; See also the 2011 report of Frank La Rue, Special Rapporteur to the Human Rights Council on the Freedom of Expression http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf

completely shut off throughout the entire country, more targeted, regional interruptions, and finally, where interruptions (and not complete shutdowns) have been put in place.

A. National shutdowns

Perhaps the most notorious example is in Egypt in 2011. On the evening of Thursday, January 27 – just two days after large-scale anti-government protests erupted across Egypt – officials in the beleaguered government of Hosni Mubarak ordered the operators of the country's main internet and mobile phone providers to “pull the plug” on their services. Egypt's four main ISPs (Telecom Egypt, Link Egypt, Vodafone/Raya, and Etisalat Misr) and its three main mobile phone companies (Vodafone Egypt, Mobinil, and Etisalat) promptly complied with this government order.

While the case in Egypt may have been the most high profile, there have been several other countries that have enacted a complete blackout of the internet. In Burma, the “Saffron Revolution” took place during the summer of 2007; intermittent internet and telephone blackouts were reported in August of that year amid mounting arrests of protesters and increased harassment of journalists. The number of sites being filtered increased, expanding to include YouTube and Blogspot. Then, between Sept. 28 and Sept. 30, a complete network shutdown occurred.⁸ Control over the internet in Burma is facilitated by the fact that the only two ISPs in Burma are both state-controlled. The two ISPs were down until October 4, and service was intermittent for the next few weeks.

B. Regional Shutdowns

There are also several examples of regional shutdowns, enacted ostensibly for the purposes of protecting public safety, or quashing undesired civic mobilization internationally (which would be a violation of international human rights law, and contrary to the statements outlined by the UN Special Rapporteur on Freedom of Expression, Frank La Rue⁹). In 2009, the Chinese government completely shut down internet service in the province of Xinjiang following ethnic riots which left close to 150 people dead and hundreds more injured.¹⁰¹¹

C. Disruptions of Service: Throttling, or “just in time blocking”

⁸ “Pulling the Plug,” <http://opennet.net/research/bulletins/013>

⁹ <http://www.ohchr.org/Documents/Issues/Opinion/A.66.290.pdf>

¹⁰ <http://opennet.net/blog/2009/07/china-shuts-down-internet-xinjiang-region-after-riots>

¹¹ <http://www.reuters.com/article/2009/07/06/us-china-xinjiang-qa-sb-idUSTRE5652FH20090706>

During the 2009 Green Revolution,¹² the Iranian government dedicated less bandwidth to internet connection providers, in addition to interrupting cell phone service. The nascent democratic movement was severely inhibited by these actions as internet traffic dropped by 54%, illustrating Iran's more subtle approach to controlling the internet, which allows it to operate – albeit at a drastically reduced speed – while utilizing the extensive state-run web-blocking and surveillance infrastructure.¹³ Libya, in the face of its own popular uprising also throttled its internet connection in many parts of the country rather than disconnecting the internet entirely.¹⁴

Access believes that throttling bandwidth is the same as shutting off the internet, as by rendering the internet unusable, the State effectively deprives its citizens of their human right to access the internet, in addition to denying their rights to freedom of expression, association, and other rights enshrined in the Universal Declaration of Human Rights.

c. What are examples of wireless networks actually being used to put the public's safety at risk? Could interruption of wireless service have mitigated these harms? How would such interruptions have mitigated these harms?

It is possible that wireless networks were utilized by the terrorists who struck in London on July 7, 2005. Authorities including the New York Police Department have alleged the bombs were detonated by mobile phones.¹⁵ However, if this were the case, and the bombs could have been set off remotely, it remains unclear as to why suicide bombers were present. However, because authorities did not expect or predict the attacks in this case, any subsequent communications interruption would not have mitigated this particular tragedy. Furthermore, as individuals increasingly turn to mobile services in emergency situations, an interruption would have the potential to cause more harm to the public than protect their safety.¹⁶

d. What existing policies do public agencies in the United States have for determining whether a service interruption is proper? What existing policies or agreements do public agencies in the United States have for effectuating an interruption of wireless service?

As mentioned in the Public Notice, NSTAC approved a communications shutdown protocol in 2006. According to NSTAC's annual reports, the National Communications

¹² http://en.wikipedia.org/wiki/2009%E2%80%932010_Iranian_election_protests

¹³ http://online.wsj.com/article/SB124519888117821213.html#mod=todays_us_page_one

¹⁴ <http://www.computerweekly.com/Articles/2011/03/07/245732/Libya-internet-blackout-continues.htm>

¹⁵ <http://news.bbc.co.uk/2/hi/4744211.stm>

¹⁶ <http://www.nij.gov/journals/261/coordination.htm>

System (NCS) approved Standard Operating Procedure 303, "Emergency Wireless Protocols (EWP)," on March 9, 2006, codifying a shutdown and restoration process for use by commercial and private wireless networks during national crises. Under the process, the National Coordinating Center (NCC) will function as the focal point for coordinating any actions leading up to and following the termination of private wireless network connections, both within a localized area, such as a tunnel or bridge, and within an entire metropolitan area. State Homeland Security Advisors, their designees, or representatives of the DHS Homeland Security Operations Center will make the decision to shutdown service.

Once the request has been made by these entities, the NCC will operate as an authenticating body, notifying the carriers in the affected area of the decision. The NCC will also ask the requestor a series of questions to determine if the shutdown is a necessary action. After making the determination that a shutdown is no longer required, the NCC will initiate a similar process to re-establish service.

At a state level, California Public Utilities Code section 7907 provides that an order to cut service may lawfully originate from a "supervising law enforcement official having jurisdiction," in a very specific situation: the officer must have "probable cause to believe that a person is holding hostages and is committing a crime, or is barricaded and is resisting apprehension through the use or threatened use of force." The carrier is protected from liability for any consequences of its "good faith reliance" on the order.¹⁷

2. Bases for interrupting wireless service. Under what circumstances, if any, is it appropriate for a public agency to interrupt wireless service? How effective is an interruption likely to be in achieving the purpose of the interruption?

Access believes that public authorities should ensure that communications networks are always maintained during emergency situations. However, even in the event of a catastrophic emergency whereby the necessary and lawful steps have been taken to officiate a interruption of wireless service, Access reminds the U.S. of its international commitments, as enshrined in the interpretation of the International Covenant on Civil and Political Rights (ICCPR), which states that to interrupt communications, a state must show "in specific and individualized fashion the precise nature of the threat, and the necessity and proportionality of the specific action taken." The purpose must be a clearly defined and legitimate public purpose. "Necessary" requires a showing of "direct and immediate connection" between the requested action and its purpose, and cannot be used to justify arbitrary or broad limitations on the right to freedom of expression.

¹⁷ <http://codes.lp.findlaw.com/cacode/PUC/1/d4/3/s7907>

Proportionality requires the interruption to be the least restrictive means required to achieve the purported aim.¹⁸

a. What types of government authorities are most likely to seek intentionally to interrupt wireless service?

As communications networks become increasingly ubiquitous, government and law enforcement authorities are more apt to seek to disrupt or shut down networks in times of emergency or, as the BART situation demonstrated, even during periods of civil unrest. It is clear that there are any number of public authorities (such as local police) who are or will likely be very keen to seek to interrupt wireless services. However, given the significant threats to human rights and civil liberties, operational control over wireless networks must remain at the highest levels of the federal government. Moreover, Access firmly maintains that the harms of shutting down wireless networks will always outweigh any benefits (see responses to Question 5 below).

b. In what kinds of situations would a government authority potentially seek intentionally to interrupt wireless service? How frequently do these situations arise? For how long would service be interrupted in these situations? How rapidly after the threat to public safety has passed can service be restored?

As touched upon in Part 1, there are a variety of potential reasons that authorities would seek to shut down or temporarily interrupt communications networks.

However, as also outlined in Part 1, a communications shutdown would rarely (if ever) benefit public safety. Indeed, there are no documented cases that Access is aware of where a network shutdown served to avert a catastrophe or was in the best interest of public safety or human rights. If in the extreme case that it was deemed necessary to shut down networks, service should be restored in a manner that does not harm the system or delay restoration of service. Services should be restored as rapidly as possible to ensure the least harm to the public who, in the aftermath of an adverse event, would need access to lines of communication, whether landline or mobile access to telecommunications networks. To minimize the risk to public safety and human rights in the event of an interruption, Access believes that citizens should always be able to access emergency services.

¹⁸ Human Rights Committee, General Comment 34, <http://www2.ohchr.org/english/bodies/hrc/docs/CCPR-C-GC-34.doc>; See also the 2011 report from Frank La Rue, Special Rapporteur to the Human Rights Council on the Freedom of Expression http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf

c. Under what circumstances would an interruption of wireless service likely be effective in protecting public safety? Under what circumstances might interrupting wireless service be ineffective?

Access believes that in the overwhelming majority of cases where communications shutdowns are considered, they are neither the most effective nor the least harmful method of protecting public safety in the face of a catastrophic or adverse situation. Access views intentional communications interruptions as akin to imposition of martial law or military takeover of real public and private property, something rarely executed in the United States, and highly circumscribed (and often criticized) when employed. It is also unlikely to be effective. By way of analogy, simply because bank robbers might predictably use city streets or cars does not justify closing those roads or outlawing vehicles. Instead, smarter policing of those avenues is more effective and productive for society.

3. Risks in interrupting wireless service. What are the risks of an interruption of wireless service? What factors affect those risks?

a. What public safety risks arise from intentionally interrupting wireless service? How are the activities of first responders and other emergency personnel and government authorities affected by an intentional interruption of wireless service? How are the activities of consumers affected by an intentional interruption of wireless service?

As outlined in previous sections, Access believes that an interruption of wireless services will always cause more harm to citizens and public authorities than good. During a time of crisis, individuals look to social media (and wireless communication in general) as a means to communicate with one another – sending photos of damage, checking the status of friends and family, or passing along news and updates about the disaster's effects. But people also look to these wireless networks for information from government agencies and companies. People may not have ready access to televisions or radios but are increasingly using mobile networks, effectively making access to the internet (and social networks for example) faster, more convenient and often more reliable than traditional forms of media. And it is not only a one-way transmission: organizations and open source software, such as CrisisCommons.org and Ushahidi, have been used during natural disasters, even in the United States, to give people the ability to easily report incidences of damage, injury or safety hazards to a centralized location where they are addressed and then swiftly responded to.¹⁹

¹⁹ <http://ushahidi.com>; see also article on the use of Ushahidi during U.S. blizzards: <http://bit.ly/zRZpsE>

Customers, therefore, would suffer greatly from any interruption of communications services. According to FCC Chairman Julius Genachowski, a majority of 9-1-1 calls – 450,000 of 650,000 daily – are now made by mobile phone users.²⁰ A survey by Pew Internet found 83% of Americans own a cell phone, and 40% of cell owners said they were in an emergency situation in which having their phone with them helped, in the 30 days before the survey.²¹

Public officials such as first responders also rely on wireless communications to accomplish their mission and ensure public safety.²² Some commentators say that ten years after the 9/11 attacks, where emergency response personnel suffered a communications breakdown, the government continues to inadequately protect wireless communications for first responders.²³

b. What are the potential economic consequences of intentionally interrupting wireless service?

National or regional economic losses stemming from an interruption of wireless services would likely be massive. Industry analysts and the Organisation for Economic Cooperation and Development (OECD) estimated that the Egyptian network shutdown cost the country at least \$110 million USD.²⁴ Telecom and internet services account for 3-4 percent of GDP in Egypt, putting the loss at about \$18 million per day, the OECD estimated shortly after the 2011 shutdown. Secondary losses of the goodwill and confidence of both domestic and foreign investors – key to the nation's economy – were no doubt harmed as well, particularly as the country had labored to lure tech companies to do business there.²⁵

The companies themselves would suffer major profit losses as well. During the Egypt shutdown, Vodafone had to hire 100 new staff in New Zealand, as its Egypt call centers were down.²⁶ Vodafone's decision to shut down its networks at the government's behest

²⁰ Prepared Remarks of Chairman Julius Genachowski, Federal Communications Commission, "Next-Generation 9-1-1," Arlington County Emergency Center Arlington, VA (9/23/2010), <http://bit.ly/J4Q8uS>.

²¹ Pew Internet, "Americans and their Cell Phones," <http://www.pewinternet.org/Reports/2011/Cell-Phones.aspx>

²² Ryan Hallahan & Jon M. Peha, "The Business Case of a Nationwide Wireless Network that Serves both Public Safety and Commercial Subscribers," 37th Telecommunications Policy Research Conference, Sept. 2009, http://www.ece.cmu.edu/~peha/profitability_of_public_safety_network.pdf.

²³ Huffington Post, "Tom Ridge: Congress Has 'Failed' 9/11 First Responders In Wireless Communications Battle," <http://huff.to/nVxH4H>

²⁴ <http://www.telecomasia.net/content/egypt-shutdown-cost-110m>

²⁵ <http://www.pcmag.com/article2/0,2817,2379324,00.asp>

²⁶ http://www.nzherald.co.nz/business/news/article.cfm?c_id=3&objectid=10703376

likely contributed to the 80 percent drop in its growth rate in Egypt during the quarter in which the shutdown occurred.²⁷ Resulting lawsuits, loss of investor confidence, and the high costs of repowering its systems likely hurt profits as well.

c. How do particular circumstances affect the risks that arise from an interruption of wireless service? Are there particular kinds of locations where interruption is especially risky? Are there areas where first responders and other emergency personnel are especially dependent upon commercial wireless service to perform their duties or where consumers are particularly dependent on wireless service? How does the availability of alternative means of communication affect the risks that arise from an interruption of wireless service? Does the interruption of wireless service pose particular risks to persons with disabilities?

Access believes that the very essence of wireless networks means that a shutdown or interruption of any kind would mean that any area is equally “risky” for public safety and for first responders (and any other emergency personnel). However, it might be especially risky in areas where there are not many pay phones, situations where stores are closed, or where people are on bridges or in tunnels, or in disabled buildings. These scenarios limit alternative communications options, and would be even more dangerous for citizens who may require emergency aid or special services. This is particularly the case for persons with disabilities.

d. What steps could be taken to minimize the risks that arise from an interruption of wireless service? What steps could be taken to narrow the scope of a service interruption?

Access firmly believes that no steps could be taken to satisfactorily minimize the risks of interrupting wireless communications, an action with innumerable, often unforeseen consequences. In the very extreme case that an interruption is deemed necessary, subject to the tests outlined above, networks should be operated in a manner that allows for the rapid restoration of service. For example, rather than cutting power to critical equipment, carriers should opt for ways to terminate the software or processes while leaving the machines running and essential personnel in place.

If an authority makes the decision to disrupt wireless service – likely a mistaken and unlawful decision – any interruption should be intentionally time-limited and geographically-specific in direct relation to the achievement of a clearly defined public purpose, as referenced in the test for restrictions on freedom of expression under the ICCPR. Moreover, restrictions should take place in as strict a manner and for as short a

²⁷ Wireless Federation, “Vodafone Growth Hit in the Wake of Riots in Egypt” <http://bit.ly/IAqByu>

duration as possible, and be limited to a very specific geographic area. Emergency services communications should never be curtailed or shutdown.

e. What institutions or officials should be notified of an intentional interruption of wireless service? How and when should they be notified? How and when should the public be notified? Should notifications include the reason for the service interruption?

All those who will be directly affected by the wireless interruption should be notified of the decision as soon as possible, and ideally in advance of any shutdown occurring. This includes, for example, chiefs of police and fire in the affected areas, state political officials including the governor and mayors of affected cities, and an SMS to all users who will be affected.

After a decision has been made to interrupt wireless communications, the public should be notified as soon as possible. This should be done through established public address and emergency alert systems and news media. For example, the existing Emergency Alert System (EAS) sends warnings to television and radio via broadcast, cable, satellite, and wireline communications pathways. The new Commercial Mobile Alert System (CMAS),²⁸ created as a partnership between FEMA, the FCC, and wireless carriers, sends Wireless Emergency Alerts (WEA) through wireless carriers across the nation. However, wireless network shutdowns or interruptions would render ineffective the CMAS, and government communications more generally, another reason against shutting down wireless networks.

f. Are there less intrusive ways of protecting public safety than interrupting wireless service? If so, what are they? Under what circumstances are these alternative means likely to be as effective as interrupting wireless service? Should government officials be required to consider alternative means before interrupting wireless service?

Almost any method of protecting public safety is less intrusive than interrupting wireless service. There are a variety of other measures that can be taken in various situations to protect public safety that do not involve shutting down wireless networks. In the BART incident, for example, wireless networks were blocked in order to prevent a public protest – however, if this were a situation where public safety was in fact at risk, BART personnel had a number of less harmful options available to them. For example, they could have ordered BART police and called on city police to guard the entrances to the

²⁸ <http://www.fema.gov/emergency/ipaws/cmas.shtm>

subways and trains. In addition, the public could have been warned of impending demonstrations and advised to make other transportation plans.

Alternative means must be considered, by law, both international and domestic, since an interruption almost necessarily derogates the U.S. obligations under treaties (the Universal Declaration of Human Rights, and the ICCPR) to respect the human rights to expression and association. Any limitation on speech and expression must be necessary and proportionate to achieve a clearly defined and legitimate public purpose. These terms are strictly construed. Any authority acting to restrict expression “must demonstrate in specific and individualized fashion the precise nature of the threat, and the necessity and proportionality of the specific action taken, in particular by establishing a direct and immediate connection between the expression and the threat.” Security threats cannot be used to justify arbitrary or broad limitations on the right to freedom of expression. Proportionality requires the government to use the least restrictive means necessary to achieve the purported aim, meaning they must consider other means of ensuring public safety than restricting speech.

g. Are there situations where the risk of interrupting wireless service will always outweigh the benefits?

In a crisis situation, interruptions will likely cause lives to be lost if people cannot connect with emergency responders. Access therefore believes that the risk of interrupting emergency communications will always outweigh the benefits. The Bureau of Public Safety and Homeland Security has noted, “any 911 call that is not connected can have serious consequences.”²⁹ Beyond emergency situations, however, Access believes interrupting wireless services would only serve to undermine and endanger human rights and public safety.

h. What kinds of liability issues for wireless service providers might be raised by wireless service interruptions?

Access strongly believes that wireless network providers should maintain control over their networks at all times, and ensure that citizens have access to these services at all times. In this way, companies could incur liability for cutting access to service when customers depend on their wireless communications in a wide range of situations, from

²⁹ Letter of Admiral James Barnett, Chief, Bureau of Public Safety and Homeland Security, to Kathleen M Grillo, Senior Vice President, Public Affairs, Policy & Communications, Verizon Communications, February 17, 2011 (inquiring as to failure of Verizon Wireless to connect over 8,000 9-1-1 calls), Bloomberg News
<http://www.bloomberg.com/apps/news?pid=conewsstory&tkr=VZ:US&sid=a7YncLZYWleA>

personal injury and emergency contexts, to breach of contract and tort damages claims by individuals and commercial enterprises.

5. Authority to interrupt service. Which public institutions, agencies, or officials have or should have the authority to request an of interruption wireless service? What process should officials with such authority use to effectuate an interruption?

Access does not believe that any authority should or could lawfully be entrusted with the power to interrupt wireless communications networks and services. Based on our review of wireless service interruptions worldwide, we further note that in no case has a government widely disrupted service in a way benefitting public safety or human rights, nor do we expect this to happen on any occasion in the future.

a. What processes could ensure that only an appropriate official makes the decision to request an interruption of wireless service? How would such an official be contacted in an emergency situation where time is of the essence?

Access firmly believes that it is not likely that any official could be “appropriately” authorized under international and domestic law to shut down wireless service networks. Furthermore, it is also not probable that such an official could be adequately briefed to make an informed decision under emergency conditions.

b. What institutions or officials should be able to review the decision to interrupt wireless service? What process considerations or safeguards should be implemented? How can timeliness of such review be ensured?

Access believes that no process considerations or safeguards will adequately remedy or address the effects of a wireless network shutdown. Damage done to public safety, the economy, human rights, and societal trust in government will likely be widespread and irreversible.

If an interruption does occur, federal courts must review the decision as soon as possible. Akin to the process of vetting an order for temporary injunctive relief, federal courts of jurisdiction should hold a hearing at the earliest possible opportunity after the interruption order has been issued. At the hearing, various experts could opine, including civil liberties, political, telecommunications, and law enforcement officials. The carrier(s) must present its actions and the estimated impact on service. Judges must consider whether the limitation on speech and expression comported with domestic and

international law, applying the test for restrictions on freedom of expression under the ICCPR as outlined above.

At the same time, immediate oversight by different branches, including the White House, the Commission, and other relevant agencies and Congressional committees is needed.

c. What obligations do or should wireless carriers have to comply with a request by a government official to interrupt wireless service?

Access believes carriers should never interrupt wireless service and should be held accountable for unlawful service interruptions. Requests from governments and partners to restrict users' access to network services, freedom of expression, or privacy should be presumptively rejected.

As noted in our Telco Action Plan (attached), before entering a market, and continuously once operating, carriers should assess the probability of a government request to interrupt service and have in place policies and procedures, along with employee training programs, to handle such requests. Prior to setting their policies -- and when updating them -- companies should consult internal and external experts on the civil and human rights pertinent to their service provision. Once a request is received, the carrier should initiate its process for vetting the request as quickly and thoroughly as possible.

A carrier must demand any request to restrict service be submitted in writing; explain the legal basis for the request; and identify the official making the request by name and title. Companies will insist that each government request to restrict service be based on a valid court order or warrant from a valid legal authority. Companies must interpret a request to interrupt service as narrowly as possible, and any compliance must take place in as strict a manner and for as short a duration as possible, and be limited to a very specific geographic area.

If a government request is unclear in its scope, or the legal basis for the request is vague, companies should interpret such requests as narrowly as possible, seek clarification from government authorities, or use such vagueness as grounds for a legal challenge to the request.

If a government request is inconsistent with local law, regulatory requirements, or contractual provisions, the request should be rejected.

d. What steps should be taken to ensure a timely return to full wireless service in the affected area? What institutions or officials should have authority to request a return to full wireless service in the affected area?

If no such procedures are already known, in its due diligence assessment, a carrier should identify shutdown procedures that least prejudice the restoration of service after an interruption. Carriers should train personnel in such benign shutdown procedures, and of course in how to reboot the system effectively and efficiently. As noted above, the procedures should strive to leave critical equipment running and personnel in place.

To reiterate, Access is adamantly opposed to any shutdown or throttling of internet and telecommunications services and believes that doing so only undermines and endangers human rights and public safety.

e. What procedures should there be to review an interruption after it has occurred?

Even if they are private corporations, carriers have duties under the United Nations Guiding Principles on Business and Human Rights,³⁰ implementing the Ruggie Framework,³¹ to respect human rights and remedy any abuses.

Full internal investigations should commence as soon as possible after any government mandated interruption. Carriers should leverage the lessons learned to remedy any deficiencies in their policies and procedures for responding to government requests. Carriers should ensure that users impacted by the network shutdown have access to appropriate remedies, including company grievance mechanisms by which to seek any requested explanations, redress, or service modifications.

In addition, the carrier should weigh its options for a response to its stakeholders, including customers, employees, and investors. Such a response could ideally include an industry-wide statement. Carriers should also advocate for the availability of public grievance mechanisms and remedies. Given their established relationship with the government, the carriers should advocate for a legal or regulatory environment that disallows or actively discourages shutdown laws and orders in favor of more effective, targeted measures.

³⁰ <http://www.ohchr.org/documents/issues/business/A.HRC.17.31.pdf>

³¹ <http://www.business-humanrights.org/Documents/RuggieHRC2008>

6. Legal constraints on interrupting wireless service. Many laws—local, state, federal, constitutional—could prohibit or constrain the ability to interrupt wireless service. The legality of an interruption could depend upon particular circumstances, such as the reason for the interruption, its duration, its geographic scope, or how the interruption is accomplished.

b. Are there circumstances under which a government entity could be construed to have common carrier obligations under the Communications Act due to its relationship with or control over wireless service?

Section 3(h) of the FCC Act defines a common carrier as “any person engaged as a common carrier for hire, in interstate or foreign communication by wire or radio.”

Additionally, a government or public entity, or a public-private mixed entity, can constitute a common carrier and incur obligations under the Communications Act.

For example, BART is a mixed public/private entity serving the public. BART controls access to wireless service for passengers in underground stations and tunnels through a network of access points, switches, and routers that connects riders with their wireless carriers. BART serves a necessary role in the provision of communications and other services to the public, in the manner of any common carrier business.

An analogy to Constitutional law is instructive as to when a public entity could be considered under the terms of private corporations. The term “market participant” is used in United States constitutional law to describe a U.S. State which is acting as a producer or supplier of a marketable good or service.³² Once their activities are sufficient to qualify them as market participants, states are treated under law as having some of the advantages and responsibilities peculiar to private corporations. What matters, then, for clarification of whether an entity is public or private are the actions it takes, rather than its constitution or governance.

If a carrier opens its doors to the public, it loses the right to discriminate unreasonably as to whom it serves – whether it is providing that service for the first time, or has done so for decades. Acting as common carriers, government entities must submit to responsibilities, including regulation, while enjoying the freedoms of private entities.

d. What protections do the First Amendment or due process rights provide for users of wireless service? Under what circumstances could an interruption of

³² *Reeves Inc. v. Stake*, 447 U.S. 429 (1980)

wireless service violate the First Amendment or due process rights of wireless users? Are there other constitutional protections that should be considered?

Access firmly believes that, in the 21st Century, safe and secure access to digital communication is a precondition to the flourishing of fundamental human rights, including the freedoms of expression and association.

A. Treaty Obligations and Supremacy Clause

The U.S. Constitution guarantees respect for these human rights. Through the Supremacy Clause of the Constitution, the United States is bound by treaties, including the International Covenant on Civil and Political Rights (ICCPR), which it has ratified. By its own language, the ICCPR is interpreted by the Human Rights Committee. Thus, the Committee's most recent interpretation, General Comment 34 (GC34), applies to the United States. Issued in 2011, GC34 interprets Article 19 of the ICCPR, which respects the freedom of expression, opinion, and access to information.

GC34 clearly foresees the need for diligence in supporting mobile communications, especially in times of crisis. In this Comment, the Committee counsels governments that the internet and mobile communications have "substantially changed communication practices around the world." In the wake of this new "global network for exchanging ideas and opinions," parties to the ICCPR "should take all necessary steps to foster the independence of these new media and to ensure access of individuals thereto." Vulnerable parties include journalists, who should be able to access disaster areas and carry out their legitimate activities -- especially in times of crisis -- the Committee writes. According to the report, "The media plays a crucial role in informing the public about acts of terrorism and its capacity to operate should not be unduly restricted." To shut off media access by closing all wireless communications during times of crisis, the U.S. government would risk violating international law and the Constitution.

B. First Amendment

U.S. courts have established protections for telecommunications users. In California, the Second District Court of Appeal has held that no state official has the authority to

suspend phone service on the mere assertion that illegal activity might take place.³³ ³⁴ New York courts have held similarly.³⁵

The First Amendment protects mobile electronic device use in public. The First Circuit Court of Appeals held in *Glik v. Cunniffe* that a man had a First Amendment right to use his cell phone to videotape the police in a public place.³⁶ The \$170,000 damages award in that case, which only affected a single cell phone user's rights, could be a harbinger of massive penalties on carriers or government officials and agencies who violate First Amendment rights of wireless communications users.

In this era of instant publication of news via mobile devices, a wireless service interruption could easily constitute an unconstitutional prior restraint on publication. Per the seminal Supreme Court case *New York Times Co. v. United States*, "the word 'security' is a broad, vague generality whose contours should not be invoked to abrogate the fundamental law embodied in the First Amendment."³⁷ That court decision leaves little room for error: "[T]he First Amendment tolerates absolutely no prior judicial restraints of the press predicated upon surmise or conjecture that untoward consequences may result."

However, to date, customers and technology users enjoy significantly fewer protections online than they do offline. It is incumbent upon the federal government to ensure that especially in times of crisis, the rights we have fought so hard for offline are protected online as well.

C. Due Process

Under the Fifth and Fourteenth Amendments, citizens may not be deprived of property without due process of law. The Supreme Court has held that due process considerations require that certain notice procedures be followed before utility service may be terminated,³⁸ including:

- Written notice must be given to the customer prior to termination of utility service.
- All written notices advising of the termination must clearly and in layman's terms inform the customer of the available opportunities to present his or her objections

³³ [People v. Brophy](#), 120 P.2d 946 (Cal. App. 1942)

³⁴ Law Journal for Social Justice, ASU, <http://bit.ly/lfdald>

³⁵ *Shillitani v. Valentine*, 184 Misc. 77 (N.Y. Sup. Ct. 1945) ("[A] telephone company may not refuse to furnish service and facilities because of a mere suspicion or mere belief that they may be or are being used for an illegitimate end; more is required.")

³⁶ http://aclum.org/sites/all/files/legal/glik_v_cunniffe/appeals_court_ruling.pdf

³⁷ <http://supreme.justia.com/cases/federal/us/403/713/case.html>

³⁸ [Memphis Light, Gas and Water Division v. Craft](#), 436 U.S. 1 (1978)

to the bill to the utility, and identify the telephone number, address, and department of the person who will handle the complaint. The opportunity for this informal hearing must be available in advance of the termination date.

- The employee or official responding to the customer communication as outlined in the written notice must have the authority to review the facts and files, to correct any errors in the billings, and arrange for credit terms.

Important for this discussion, the Court found that, “Although utility service may be restored ultimately, the cessation of essential services for any appreciable time works a uniquely final deprivation.”³⁹ Though the technology may have changed since this 1978 decision, the logic remains that telecommunications customers have ample due process concerns and protections under the U.S. Constitution. Without providing adequate notice of a service interruption, the government risks impinging on a right that cannot easily be compensated for.

e. What protections do the First Amendment, due process, or other constitutional rights afford wireless carriers? Under what circumstances could a forced interruption of wireless service violate the First Amendment, due process, or other constitutional rights of wireless carriers?

Under *Citizens United v. Federal Elections Commission*,⁴⁰ corporations are extended First Amendment protections. They must not be forced to speak or endorse any political position or other message against their will, even if the government is mandating the speech under a valid law or legal purpose. See *Hurley v. Irish American Gay, Lesbian, and Bisexual Group of Boston*, 515 U.S. 557 (1995).⁴¹ Forcing a service provider to shut down during a political event like a public demonstration could be seen as forced silence. This forced silence or omission could constitute an unlawful limitation on speech, or coerced endorsement of a message, violating *Citizens United* and *Hurley*. The case for a service provider’s First Amendment rights becomes even stronger when that provider explicitly guarantees to respect the rights of its customers to speak and access its networks freely, as through its Terms of Service.

The Due Process clause of the Fifth Amendment, as applied to states through the 14th Amendment, decrees corporations may not be deprived of property without due process of law. See *Smyth v. Ames*, [169 U.S. 466, 522](#), 526 (1898); *Kentucky Co. v. Paramount Exch.*, [262 U.S. 544, 550](#) (1923); *Liggett Co. v. Baldridge*, [278 U.S. 105](#) (1928). Corporate profits lost due to any interruption could be calculated by carriers and directly

³⁹ 436 U.S. at 20. See also *Stanley v. Illinois*, 405 U. S. 645 (1972)

⁴⁰ 558 U.S. ____ (2010)

⁴¹ http://en.wikipedia.org/wiki/Hurley_v._Irish-American_Gay,_Lesbian,_and_Bisexual_Group_of_Boston

attributed to the mandated service interruptions. Courts could force the government to compensate companies for massive losses.

Telecommunications companies are almost always common carriers and therefore must not unreasonably discriminate in services offered to the public, per 47 U.S.C. § 202. Thus, they are open to liability for shutting off certain customers. But carriers found to have violated users' rights may have redress against the public officials who ordered the interruptions under Section 1983 of title 42 of the U.S. Code. Part of the Civil Rights Act, §1983 could be an avenue for carriers to recover damages awards that are forced to pay to their affected customers. If municipalities indemnify public officials for §1983 punitive damages awards, those municipal treasuries could be forced to pay large amounts.

f. What provisions of Title II of the Communications Act prohibit or circumscribe an interruption of wireless service, and under what circumstances? To what extent do sections 202, 214, 302a, 333, or other sections of the Communications Act circumscribe the ability of government actors to interrupt wireless service?

Section 333 prohibits any person from willfully interfering with any station licensed or otherwise authorized under the Act. Any authority granted to public or private officials to interrupt service must therefore explicitly override this provision.

Section 214(a) prohibits network operators from discontinuing or impairing service without prior authorization from the Commission. Any authority granted to carriers and network operators to interrupt service without Commission authorization must therefore explicitly override this provision.

Section 615 encourages states to create "comprehensive end-to-end emergency communications infrastructure," with "seamless, ubiquitous, reliable wireless telecommunications networks and enhanced wireless 9-1-1 service." Clearly, any intentional interruptions to emergency or other wireless services would contradict the stated goals of the Commission under this provision and likely lead to confusion in affected states.

g. What state laws prohibit or circumscribe an interruption of wireless service? What authorities do state public utility commissions have to prohibit or circumscribe an interruption of wireless service? Are there circumstances in which approval of a state public utilities commission is necessary before ordering a shutdown?

California State Senate Bill SB1160 is attempting to impose additional safeguards for First Amendment concerns against any communications shutdown order.⁴²

h. To what extent does a public agency's contractual or practical control over wireless service equipment affect the analysis of whether a public agency has the legal authority to interrupt wireless service?

The extent of a public agency's control over the equipment is *not* determinative as to whether that entity has the authority to effectuate a communications interruption. However, it could constitute a factor in deciding that the company was acting at the direct behest of the state, in which case full Constitutional protections (and associated remedies) could apply to all those affected by the state action.

Forcing a company to install, operate, and maintain equipment or software necessary to affect such an interruption could well constitute a Constitutional taking under the Due Process clauses of the 5th and 14th Amendments. In these cases, the government must provide adequate compensation, which could be extremely expensive.

i. What is the scope of the Commission's discretion to set policies that affect a public agency's legal authority to interrupt wireless service? To the extent the Commission has not exercised this discretion, should it do so, and in what ways?

It should be noted that a federal shutdown order may violate the 10th Amendment. The federal government cannot commandeer state law enforcement officials to carry out its laws.⁴³ If the Commission were to use state law enforcement to effect a shutdown, it may qualify under *Printz* as "forced participation of the State's executive in the actual administration of a federal program." This is unconstitutional, even for a temporary program or action.

States do not have authority under the Commerce Clause to regulate interstate communications. Modern wireless communications are interstate communications. Thus, only the FCC can regulate wireless communications. It is the FCC's responsibility, therefore, to see that no customers are deprived of their rights to expression, access to information, and association.

⁴² See the Bill at <http://1.usa.gov/lh5PO3> "Bill bars cell service shutdown by public agencies," San Francisco Chronicle, <http://bit.ly/HQruMM>

⁴³ *Printz v. United States*, 521 U.S. 898 (1997)